#31

National Association of Manufacturers

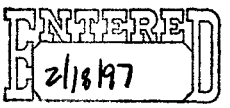
oward Lewis

Vice President

Trade & Technology Policy

February 13, 1997

Nancy Crowe
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
Room 2705
14th Street and Pennsylvania Ave., NW
Washington, DC 20230



RE: 15 CFR Parts 730, 732, 734, 736, 738, 740, 742, 744, 748, 750, 768, 772, and 774

Dear Ms. Crowe:

The National Association of Manufacturers (NAM) is pleased to offer its comments on the interim rule on Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List, 61 *Federal Register* 68572-87 (Dec. 30, 1996). The NAM, representing 14,000 companies producing 85 percent of America's manufactured output, is the nation's oldest and largest broad-based trade association.

Policy Immobility Versus Rapid Global Change

The NAM appreciates that the government has undertaken the transfer of jurisdiction of this subject matter from military to civilian control, a move that is both welcome and long overdue. At the same time, the interim final rule represents the continuance of burdensome U.S. controls on encryption products not negotiated with our allies. A viable international regime directed toward encryption needs to meet two fundamental conditions: Various national policies need to acknowledge, indeed promote, the prudent use of encryption by private parties to protect their own assets against loss; and such national policies need to be harmonized so as to avoid market-distorting disparities. The NAM submits that neither condition is met in the current policy.

Without question, the manufacturers' need to employ end-to-end computer network security measures is on the rise. The just-released *Next-Generation Manufacturing Report* – sponsored notably by four federal agencies, including the departments of Defense, Commerce and Energy, as well as numerous trade associations – establishes the concept of the "extended enterprise." To go beyond quality management and to transcend today's dilemmas, companies in various supply chains will find themselves teaming and partnering intensively, sending data back and forth for R&D, product development and coordinated just-in-time deliveries. Such data will have to be secured. Companies need the entrepreneurial freedom to choose what security measures to employ or not to employ, just as they make countless other choices as to inputs or factors of production.

Notably, this policy change falls far short of what the National Research Council called for last year after the fullest, most intense study of encryption policy yet conducted:

> Recommendation 2 – National cryptographic policy should be developed by the executive and legislative branches on the basis of open discussion and governed by the rule of law.
>
> Recommendation 3 – National cryptography policy affecting the development and use of commercial cryptography should be more closely aligned with market forces. National cryptography policy has become increasingly disconnected from market reality and the needs of parties in the private sector. Experience with technology deployment suggests that reliance on market forces is generally the most effective way to promote the widespread use of a new technology. National cryptography policy should align itself with user needs and market forces to the maximum feasible extent.
>
> Recommendation 4.1 – Products providing confidentiality at a level that meets most general commercial requirements should be easily exportable. Today, products with encryption capabilities that incorporate the 56-bit DES algorithm provide this level of confidentiality and should be easily exportable.
>
> Recommendation 4.3 – The U.S. government should streamline and increase the transparency of the export licensing process for cryptography. (Computer Science and Telecommunications Board, National Research Council, *Cryptography's Role in Securing the Information Society*, May 1996).

While the council documented its findings and recommendations at book length, this rule also provides no sound underpinning for its primary content, the new rules regarding key escrow or key management infrastructure. To the contrary, the policy constitutes a top-down mandate that the only U.S.-origin encryption product that can be used internationally is key-recovery product, for which market demand has yet to be demonstrated and which does not yet even exist. The NAM objects to the burdensome new licensing requirements as not justified by any sound, accepted principle of export-control policy and calls instead for the de-control of encryption technology up to the 56-bit level as recommended by the National Research Council.

Moreover, the U.S. Government has not succeeded in convincing key allies – Japan, for example -- to impose similar restraints on their firms, which are the competitors of NAM members. U.S. industry has borne decades of U.S. export controls on dual-use technology not matched by even our closest politico-military allies, but left instead to "national discretion" under which the U.S. has chosen to prevent exports, but other nations have chosen to approve them. This unbroken history lends no credence to the belief that these allies will soon match these U.S. restraints. Indeed, the best current estimate of annual sales losses to U.S. firms from U.S. export controls, by the Institute for International Economics, is $30 billion.

Moreover, advanced cryptographic product is available from countries outside the set of allies that have cooperated on export controls in the past. The government has offered no credible way to cut off the availability of non-key recovery products. Manufacturers will face a variety of security contexts, ranging from stored data to transmitted data, and from symmetric block ciphered data to

asymmetric public-key ciphered data. Patterns of preference may emerge as to when and where manufacturers decide they need and want key recovery for their own purposes. As manufacturers take mission-critical applications abroad, however, they will be precluded from relying on U.S. information technology vendors for non-key-recovery solutions where those are believed sufficient. The only sure immediate result from such impositions on U.S. information technology vendors, inevitably, will be loss of sales to them and the constriction of choice by customers such as manufacturers.

Two Rules or One Rule?

This notice constitutes the second of what must be seen as a pair of regulatory notices, the first being the interim rule for Licensing of Key Escrow Encryption and Software, 61 *Federal Register* 65462-67 (Dec. 13, 1996). The NAM does not understand why two separate notices were issued, with attendant confusion, and calls on the Department of Commerce to clarify that the first rule, not acknowledged in the second, is entirely subsumed by the second. The NAM urges clarification quickly so that there can be no doubt that the second notice explicitly supersedes the first in general, and in particular that foreign-based escrow agents are not *per se* unacceptable. If the later rule entirely subsumes and supersedes the earlier one, why does it not say so?

Continuing Controls on Publicly Available Technology

In the List of Items Controlled, Section 734.3(b)(3) gives with one hand and takes away with the other. "Publicly available technology and software" are excluded from coverage under the Export Administration Regulations (EAR), "except software controlled for EI [Encryption Items] reasons." That is, encryption software is excepted from the exception and therefore covered. The new section indicates that the department will be attempting -- with what degree of overall success remains to be seen -- to maintain controls on even publicly available key escrow encryption software. The worldwide spread of the Pretty Good Privacy (PGP) program via the Internet, even when not originally so intended by its author, indicates that the department will have little success.

More fundamentally, this provision stands at odds with the recent federal district court ruling in California in *Bernstein vs. United States*, in which the court, putting its finger on the matter, characterized the attempt to maintain export controls in these circumstances as a "paradigm of standardless discretion." The department's notice curiously makes no reference at all to the litigation. Rather, the government should state its intention clearly regarding the outcome of this litigation. The provision in question is impossible to enforce effectively as a practical matter, and is of highly dubious constitutionality at best under the First Amendment. The government proposes to stop Americans from communicating abroad – or even to foreigners domestically – information that is neither classified nor proprietary and which, like any other protective device from conventional locks to car alarms, enables any party to protect its assets. That is, the information in question is in the public domain and has a *prima facie* valid civilian and commercial use. The government is not succeeding in its attempts to justify this policy in court, has not succeeded in sequestering such information to date on the Internet, and should simply drop this provision.

Technical Matters

Three technical points deserve mention. First, the notice repeatedly uses the term "manufacturers" in a highly limited and misleading way, contrary to the department's own oft-cited statistic that there are 380,000 manufacturing firms in the United States. Only some fraction of one percent of all those firms would qualify as "manufacturers" in the limited sense of the notice, that of being a primary information technology vendor. However, the new, but still highly restrictive, policy primarily affects manufacturers generally in that it stands in the way of their achieving a global agile enterprise business model with ever closer ties with suppliers and customers.

Paragraph (3) of the background discussion exemplifies the confusion. It begins with the phrase "Manufacturers of non-recovery encryption items" as the only reference to manufacturers. Later on it states, "BXA will accept requests for classification from distributors, re-sellers, integrators and other entities that are not manufacturers of the encryption items." The first use of "manufacturers" could be well substituted by "vendors," and the list of parties should be expanded to include manufacturers, generally and properly considered.

Second, the notice imports the definition of "mass market software" that was originally arrived at in negotiations of the former Coordinating Committee on Export Controls (CoCom) before the rise of the Internet and its World Wide Web (Supplement No. 2 to Part 774, II. General Software Note). It therefore must be updated to reflect the new business practice of delivering software by downloading.

Third, Note c, following item g in the list of items controlled under 5A002, could benefit from improved wording: "Receiving equipment for radio broadcast, pay television or similar restricted audience television of the consumer type, without digital encryption and where digital decryption is limited to the video, audio or management functions." Since the category is limited expressly to receiving equipment in the first place, the inclusion of the "without digital encryption and" phrase becomes confusing, and the language would be both unambiguous and better without it. If "receiving" is not felt to be limiting enough, then we suggest "Receive-only."

Conclusion

While the new policy represents an improvement, it still falls far short of what the National Research Council has recommended. The government has presented no reason not to accept its recommendation to de-control encryption capability up to the 56-bit level. Accordingly, the NAM calls for such de-control.

Sincerely,

Howard Lewis

Howard Lewis
Vice President,
Trade and Technology Policy